IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): J.A. Garay et al.
Case: 8-32
Serial No.: 10/014,763
Filing Date: December 11, 2001
Group: 2132
Examiner: Samson B. Lemma

Title: Method and Apparatus for Computationally-Efficient Generation of Secure Digital Signatures

---

REPLY BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The remarks which follow are submitted in response to the Examiner's Answer dated July 13, 2006 in the above-identified application. The arguments presented by Applicant (hereinafter "Appellant") in the Appeal Brief dated April 24, 2006 are hereby incorporated by reference herein.

Appellant will respond herein to certain arguments raised by the Examiner in Section (10), pp. 10-16, of the Answer.

At pp. 11 and 12 of the Answer, the Examiner argues that dependent claim 3 of the present application is indefinite under 35 U.S.C. §112. More specifically, the Examiner argues that the limitation "having a computational efficiency lower than that of the first digital signature protocol" must be quantified in order to be made statutory. Appellants respectfully disagree. One skilled in the art will recognize that computational efficiency is ordinarily and customarily an indicator of how much time a computational device requires to perform a given function. Indeed, such a definition is

supported in the Specification at, for example, p. 1, ll. 18-22 and p. 7, ll. 3-8. As a result, one skilled in the art will further recognize that a second digital signature protocol has a computational efficiency lower than that of a first digital signature protocol if the second digital signature protocol requires more time to determine than the first digital signature protocol on a given computational device. Appellants, therefore, respectfully submit that the scope of claim 3 would be clear to one skilled in the art in light of the ordinary and customary meanings of the words in the claim and their usage in the Specification.

Moreover, at pp. 12-14 of the Answer, the Examiner argues that independent claim 1 of the present application is anticipated by Aura under 35 U.S.C. §102(e). More specifically, the Examiner argues that Aura's "authentication centre" describes the claimed "user device." What is more, the Examiner argues that Aura's "mobile station" describes the claimed "intermediary device." Appellants respectfully submit that both assertions are untenable.

In asserting that Aura's "authentication centre" describes the claimed "user device," the Examiner argues that the claimed "user device" is defined in the Specification at p. 5, ll. 11-16 which states that a user device "may alternatively be implemented in a desktop or portable personal computer, a wearable computer, a television set-top box or any other type of device capable of transmitting or receiving information over network 104." Nevertheless, while this description does in fact provide examples of various user devices, it does not include devices not associated with a user within the definition of user devices, as the Examiner would seem to argue. This becomes clear by reading the paragraph from which the above-quoted language is taken in its entirety. The paragraph states:

> Although illustrated in this embodiment as a mobile telephone or PDA, the user device 102 may alternatively be implemented as a desktop or portable personal computer, a wearable computer, a television set-top box or any other type of device capable of transmitting or receiving information over network 104. In addition, there may be multiple such devices associated with a given user. For example, a given user may have a mobile telephone as well as a desktop or portable computer, and may utilize both devices for signature generation.

Specification, p. 5, ll. 11-16 (*emphasis added*). From this description, as well as the usage of the term "user device" throughout the remainder of the Specification, one skilled in the art will recognize that a user device, in conformity with its plain meaning, is a device operated by a user. As a result, Aura's authentication centre does not describe the user device of claim 1 since an authentication centre is not operated by a user. See, e.g., Aura, FIG. 1; col. 1, ll. 38-59; col. 5, ll. 21-51 (Authentication centre is a fixed element in a network and performs tasks related to authenticating the identity of the network).

Furthermore, when asserting that Aura's mobile station describes the claimed intermediary device in claim 1, the Examiner argues that Aura's mobile device acts on a signature generated by a user device. Examiner's Answer, p. 14. Appellants again respectfully disagree. The mobile station is itself the user device in Aura's telecommunications system. See, e.g., Aura, col. 1, ll. 49-59 (Mobile station is operated by a mobile subscriber).

Consequently, Aura fails to describe each and every element of claim 1.

Finally, at pp. 15 and 16 of the Answer, the Examiner states that the Appellants rely solely on the patentability of the independent claims for the patentability of the dependent claims. This is incorrect. In the Appeal Brief, Appellants assert that dependent claims 3-7, 9, 10 and 17 are separately patentable over the primary §102(e) reference, Aura. Moreover, Appellants assert that the §103(a) rejections of dependent claims 8, 11-16 and 18 are deficient. Appellants therefore respectively disagree with the Examiner's assertion that all the dependent claims should stand or fall with their respective independent claims.

For the reasons identified above and in the Appeal Brief, Appellants respectfully submit that claims 1-25 are in condition for allowance, and respectfully request the withdrawal of the §§112, 102(e) and 103(a) rejections.

Respectfully submitted,

Date: September 11, 2006

Michael L. Wise
Attorney for Applicant(s)
Reg. No. 55,734
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2722